I·C·A·C

INDEPENDENT COMMISSION AGAINST CORRUPTION

NEW SOUTH WALES

NSW INDEPENDENT COMMISSION AGAINST CORRUPTION

NSW ICAC Data Breach Policy

November 2023

Contents

1 Introduction

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) ("the PPIP Act") establishes the NSW Mandatory Notification of Data Breach Scheme ("the MNDB Scheme").

The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify the NSW Privacy Commissioner and, in certain cases, affected individuals of eligible data breaches.

Under the MNDB Scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

This DBP outlines the approach of the NSW Independent Commission Against Corruption ("the ICAC") to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

2 Scope

This policy applies to all staff and contractors of the ICAC. This includes temporary and casual staff, private contractors and consultants and any other authorised person accessing ICAC systems, networks and/or information.

This policy will be reviewed and updated annually or where improvements are identified in response to a data breach, whichever occurs sooner.

3 Purpose

The purpose of this DBP is to provide guidance to ICAC staff on data breaches of ICAC-held data in accordance with the PPIP Act.

This DBP sets out how the ICAC will respond to data breaches involving personal information. The ICAC acknowledges that not all data breaches will be eligible data breaches but, regardless, the ICAC takes all data breaches seriously. The DBP details:

- what constitutes an eligible data breach under the PPIP Act
- the roles and responsibilities for reporting, reviewing and managing eligible data breaches
- the steps involved in responding to an eligible data breach and reviewing systems, policies and procedures to prevent future data breaches.

4 Definitions

- **Affected individual –** an individual specified in subsection (1)(a) or (1)(b)(ii) of s 59D of the PPIP Act.
- **Approved form** – the form approved by the Privacy Commissioner under s 59ZH of the PPIP Act.
- **Assessment –** the assessment required under s 59E(2)(b) of the PPIP Act, being an assessment of whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach.
- **Assessor** – a person or team directed by the Chief Executive Officer (CEO) to carry out an assessment of a data breach (s 59G of the PPIP Act).
- **Eligible data breach** – under s 59D(1) of the PPIP Act, this means:

  (a) there is unauthorised access to, or unauthorised disclosure of, personal information held by the ICAC and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or

  (b) personal information held by the ICAC is lost in circumstances where

    (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

    (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in ***serious harm*** to an individual to whom the information relates.
- **Held** – personal information is held by the ICAC if

  (a) the ICAC is in possession or control of the information, or

  (b) the information is contained in a state record in respect of which the ICAC is responsible under the *State Records Act 1998* (s 59C of the PPIP Act).
- **Personal information** – information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion (s 4 PPIP Act). In this policy, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002* ("the HRIP Act") and includes information about an individual's physical or mental health, or disability, or information connected to the provision of a health service to an individual.
- **Serious harm** – this is not defined in the PPIP Act but involves harm that can arise as the result of a data breach and will vary based on:
  - the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
  - the level of sensitivity of the personal information accessed, disclosed or lost
  - the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the ICAC discovering the breach.
  - the circumstances of the individual(s) affected and their vulnerability or susceptibility to harm.

5 Roles and responsibilities

Everyone to whom this policy applies is responsible for:

- ensuring that they have read this policy and the Data Breach Response Plan and that they understand what is expected of them
- complying with the PPIP Act and HRIP Act including protecting personal information held by the Commission from unauthorised access, disclosure or loss
- immediately reporting a data breach or suspected data breach to their manager, who then reports it to the CEO.

The CEO (or other person delegated the relevant functions by the CEO) is responsible for:

- assessing the severity of data breaches involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates, and notifying the Privacy Commissioner, affected persons and others where required
- immediately reporting all data breaches that are also cyber security incidents to the Principal Information Security Officer if they have not already been reported.

The Manager Communications and Media will provide advice on any communication strategy and messaging to affected individuals and external reporting agencies.

6 How the ICAC has prepared for a data breach

The ICAC has established a range of systems and processes for preventing and managing data breaches, including the following:

- Scheduling annual review and updating of this DBP, or more frequent review and updating if needed.
- Implementing a cyber security awareness program.
- Implementing a requirement for all staff to classify information consistent with the NSW Government information classification and labelling guidelines.
- Implementing a suite of cyber security policies, standards, procedures, and guidelines.
- Regularly exercising the Cyber Incident Response Plan, including participation of the ICAC Executive and relevant staff.
- Implementing a requirement for all ICAC staff to complete training in the areas of cyber security and the NSW data breach notification requirements.

7 Eligible data breaches

An eligible data breach is defined in s 59D(1) of the PPIP Act (see above).

A data breach can be caused in various ways, including as the result of malicious action, systems failure or human error.

Examples of data breaches include:

- When a letter or email is sent to the wrong recipient.
- When system access is incorrectly granted to someone without appropriate authorisation.

- When a physical asset such as a paper record, laptop, USB stick or mobile telephone containing personal information is lost, misplaced or stolen.
- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to, or theft of, personal information.
- Employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

Serious harm occurs where the harm arising from the eligible data breach has resulted, or may result, in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm, economic, financial or material harm, emotional or psychological harm, reputational harm, and other forms of serious harm that a reasonable person in the ICAC's position would identify as a possible outcome of the data breach.

8 Reporting and responding to a data breach

The CEO must be informed of any data breach to ensure the application of this DBP, including making notifications to the Privacy Commissioner for eligible data breaches and, where relevant, affected individuals.

There are five key steps required in responding to a data beach:

1. Initial report and triage
2. Contain the breach
3. Assess and mitigate
4. Notify
5. Review

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. Step five involves recommendations for longer-term solutions and prevention strategies.

Step one: Initial report and triage

A staff member is to notify their manager as soon as possible but, in any event, within one business day of becoming aware that a data breach has occurred and provide information about the type of data breach.

A contractor or third-party provider is to notify the senior ICAC manager to whom they report within the above time. The manager will notify the CEO immediately of a suspected eligible data breach.

The CEO will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme, complete the Data Breach Report and Action Plan and include all data breaches in the Internal Data Breach Register and appoint an internal Assessor.

Members of the public are also encouraged to report any data breaches to the ICAC in writing by using the contact options available on our website (www.icac.nsw.gov.au).

Step two: Contain the breach

The ICAC prioritises containing the breach.

All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords.

If a third party is in possession of the data and declines to return it, it may be necessary for the ICAC to seek legal or other advice on what action can be taken to recover the data.

When recovering data, the ICAC will make sure that copies have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third party that the copy of the data that they received in error has been permanently deleted.

Step three: Assess and mitigate

To determine what other steps are needed, the ICAC will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme, and the risks and potential for serious harm associated with the breach.

The Assessor carrying out the assessment will consider the matters set out in s 59H of the PPIP Act.

The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response.

Data Breach Report and Action Plans are to be saved in the ICAC's electronic recordkeeping system. The CEO will be responsible for the implementation of proposed actions and recommendations.

Some types of data are more likely to cause harm if compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list. Given the ICAC's statutory functions, release of complaint- and investigation-related personal information will be treated very seriously. A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft). Factors to consider include:

- **Who is affected by the breach?** Assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- **What was the cause of the breach?** Assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Questions include: Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?
- **What is the foreseeable harm to the affected individuals/organisations?** Assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue, if it could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to an individual and/or damage the ICAC's reputation?
- **Guidance issued by the Privacy Commissioner on assessing eligible data breaches** Upon becoming aware of a possible data breach, the ICAC will take into account any guidance issued by the Privacy Commissioner.

An assessment is to be carried out in an expeditious way and, in any event, within 30 days of the ICAC becoming aware of the data breach (s 59E of the PPIP Act). The CEO may, if satisfied the assessment cannot reasonably be conducted within 30 days, approve an extension of the period in which to conduct the assessment. An extension may be approved for an amount of time reasonably required for the assessment to be conducted (s 59K of the PPIP Act).

If an extension is approved, the CEO must give written notice to the Privacy Commissioner (s 59K(3) of the PPIP Act).

If the assessment is not conducted within the extension period, the CEO must provide written notice to the Privacy Commissioner in accordance with s 59K(4) of the PPIP Act.

In order to mitigate a breach, the ICAC will consider the following measures:

- Implementation of additional security measures within relevant ICAC systems and processes to limit the potential for misuse of compromised information.
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites.
- Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes.

Step four: Notify

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered.

There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form, a copy of which is attached to this DBP (s 59M(1) of the PPIP Act).
2. Determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, the ICAC may not be required to notify affected individuals. Exemptions apply in relation to:
    a) eligible data breaches of multiple public sector agencies, where one of the agencies has already notified the eligible data breach (see s 59S of the PPIP Act)
    b) where notification would likely prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal (see s 59T of the PPIP act)
    c) where the ICAC has taken certain action with respect to the eligible data breach (see s 59U of the PPIP Act)
    d) where compliance by the CEO would be inconsistent with a secrecy provision of an Act or statutory rule that prohibits or regulates the use or disclosure of information (such as s 111 of the *Independent Commission Against Corruption Act 1988* ("the ICAC Act") – see s 59V of the PPIP Act)
    e) where the CEO considers notification would create a serious risk of harm to an individual's health or safety (see s 59W of the PPIP Act)
    f) where the CEO considers notification would worsen the ICAC's cyber security or lead to further data breaches (see s 59X of the PPIP Act).
3. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
4. Provide further information to the Privacy Commissioner.

ICAC exemption from notifying individuals

In the case of the ICAC, s 111 of the ICAC Act will be relevant in relation to the exemption under s 59N of the PPIP Act to notify individuals. In each case, the CEO should consider whether compliance would be inconsistent with that section and, where compliance would be inconsistent, whether a direction should be sought from an ICAC Commissioner pursuant to s 111(4)(c) of the ICAC Act to permit disclosure of particular information.

The ICAC recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations. Notification demonstrates a commitment to open and transparent governance and it may therefore be in the public interest for a direction to be made pursuant to s 111(4)(c) of the ICAC Act.

If a data breach is not an eligible data breach under the MNDB Scheme, the CEO may still consider notifying individuals/organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systemic issues and the ability of the individual to take further steps to avoid or remedy harm.

When to notify individuals

Where individuals are to be notified, the notification should be undertaken promptly to help avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable. The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. While this DBP sets a target of notification within **five (5)** working days, practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, the ICAC will consider issuing a public notification on its website.

How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person.

Indirect notification – such as information posted on the ICAC website, on its social media channels, or a media release – should generally only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).

A record of any public notification of a data breach will be published on the ICAC's website and recorded on the Public Data Breach Register for a period of 12 months.

What to say

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

1. The date the breach occurred.
2. A description of the breach.
3. How the breach occurred.
4. The type of breach that occurred.
5. The personal information included in the breach.
6. The amount of time the personal information was disclosed for.
7. Actions that have been taken or are planned to secure the information, or to control and mitigate the harm.
8. Recommendations about the steps an individual should take in response to the breach.
9. Information about complaints and reviews of agency conduct.
10. The name of the agencies that were subject to the breach.
11. Contact details for the agency subject to the breach or the nominated person to contact about the breach.

Other obligations including external engagement or reporting

The CEO will notify the Solicitor to the Commission of any eligible data breaches so that the Solicitor to the Commission can inform the ICAC Inspector.

The CEO will report any eligible data breaches to the Principal Governance and Risk Officer as well as the ICAC's Audit and Risk Committee.

The CEO will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), when a data breach occurs. Depending on the circumstances of the data breach this could include:

- the NSW Police Force and/or Australian Federal Police, where the ICAC suspects a data breach is a result of criminal activity
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and the Australian Cyber Security Centre, where a data breach is a result of a cyber security incident or involves malicious activity from a person or organisation based outside Australia
- the Office of the Australian Information Commissioner, where a data breach may involve agencies under federal jurisdiction
- any third-party organisations or agencies whose data may be affected
- financial services providers, where a data breach includes an individual's financial information
- professional associations, regulatory bodies or insurers, where a data breach may have an impact on these organisations, their functions and their clients.

Step five: Review

The CEO will further investigate the circumstances of the breach to determine all relevant causes and consider what short- or long-term measures could be taken to prevent any reoccurrence. Depending on the nature of the breach, step five may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three above.

Preventative actions could include a:

- review of the ICAC's IT systems and remedial actions to prevent future data breaches
- security audit of both physical and technical security controls
- review of relevant policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be approved by the CEO. Consideration will also be given by the CEO to reporting relevant matters to the ICAC's Audit and Risk Committee

9 Communication strategy

The Manager Communications and Media is responsible for all communications issued under this DBP.

The ICAC aims to notify affected individuals, and external reporting agencies within five (5) business days of a data breach of ICAC-held information being reported to the IPC. Notifications to individuals will have regard for this DBP as well as the ICAC's Privacy Management Plan. Where engagement with external reporting authorities is required, the CEO and Manager Communications and Media and other ICAC Executive Team members are included as required.

10 Related documents

This policy should be read with the:

- ICAC Privacy Management Plan
- *Privacy and Personal Information Protection Act 1998*
- ICAC Cyber Incident Response Plan and Data Breach Playbook
- ICAC Business Continuity Plan
- ICAC Risk Management Policy

11 Contacts

ICAC officers should report any eligible data breach to their manager, who subsequently reports the breach to the CEO.

Members of the public or other persons who are not ICAC officers should report any eligible data breach by email to , which will be forwarded to the CEO.

A copy of the Information and Privacy Commission's Mandatory Data Breach Reporting Form – Data Breach Notification to the Privacy Commissioner is attached. The writable version of the form can also be accessed here.

12 Document Control

Version	Identification number	Date approved	Approved By	Review date
1.0	D10936863	29 November 2023	CEO	24 November 2024

July 2023

Mandatory Data Breach Reporting Form

Data Breach Notification to the Privacy Commissioner

Section 59M of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires the head of a public sector agency to immediately notify the Privacy Commissioner of an eligible data breach using an approved form. This form has been approved by the Privacy Commissioner for use by agencies for the purpose of notification under section 59M of the PPIP Act.

This approved form sets out the information that agencies must supply to the Privacy Commissioner when making a notification of an eligible data breach, unless it is not reasonably practicable to provide that information.

This document is not to be used for agency's notification to individuals affected by a breach, however the information supplied may be of use when developing your agency's written notification as required by section 59N of the PPIP Act.

Agency making notification

Agency name:

Agency address:

Telephone number:

Contact name:

Contact telephone:

Contact email:

Contact role/title in organisation:

Notification made on behalf of another agency/agencies (if applicable)

Is the notification made on behalf of another agency/agencies? Yes ☐ No ☐

If yes, complete the agency details below:

Name:

Address:

Telephone number:

Contact name:

Contact telephone:

Contact role/title in organisation:

If the notification is made on behalf of more than one agency, please provide the above details for each agency as a separate attachment.

Type of personal information that was the subject of the breach

Select the option(s) that best apply:

☐ Contact details

☐ Identity documents/credentials

☐ Financial information

☐ Health information

☐ Under review (agency is still conducting its assessment at time of notification)

☐ Other sensitive information:

Description of eligible data breach

Discovery of the breach

When the data breach occurred:

When the data breach was discovered:

Where the data breach was discovered:

How the data breach was discovered:

By whom was the data breach discovered:

Amount of time the personal information was exposed:

Type of breach

Select the **type(s) of data breach** as applicable:

☐ Unauthorised disclosure

☐ Unauthorised access

☐ Loss of information

☐ Other:

How the breach occurred

Provide a brief explanation as to how the breach occurred:

Cause of breach

☐ Cyber Incident

If the breach was caused by a Cyber Incident, select the type of Cyber Incident below:

☐ Ransomware

☐ Malware

☐ Phishing (compromised credentials)

☐ Compromised credentials (method unknown)

☐ Hacking

☐ Brute Force Attack (compromised credential)

☐ Other:

☐ Human Error

☐ Loss/theft of data/equipment

☐ System fault

☐ Other:

Remedial action taken to date (including description of action and when)

Remedial action to be taken

Notification to affected persons

Total number of individuals affected, or likely to be affected by the breach (provide best estimate if exact figure is unknown):

Total number of individuals notified of the breach at this stage:

Total number of individuals yet to be notified of the breach:

Provide details of how and when individuals were notified:

Have individuals been advised of the complaints and internal review procedures under the PPIP Act?

Recommendations made to affected individuals about the steps they should take to mitigate the effects of the breach

Estimated cost

Estimated cost of the breach to the agency:

Other bodies notified

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au